DOCKET NO: U 015993-0
INT'L. APPLN. NO.: PCT/CN2003/000305
INT'L. FILING DATE: 25 APRIL 2003
SERIAL NO: 10/554,304

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/20

A1

(11) International Publication Number: WO 00/03553

(43) International Publication Date: 20 January 2000 (20.01.00)

(21) International Application Number: PCT/US99/15174

(22) International Filing Date: 1 July 1999 (01.07.99)

(30) Priority Data:
09/112,071 8 July 1998 (08.07.98) US

(71) Applicant *(for all designated States except US)*: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: WEST, Terry, D. [CA/US]; 728 N. May Street, Chandler, AZ 85226 (US). ENGLAND, David, G. [GB/US]; 1505 W. Honeysuckle Lane, Chandler, AZ 85248 (US).

(74) Agents: MILLIKEN, Darren, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

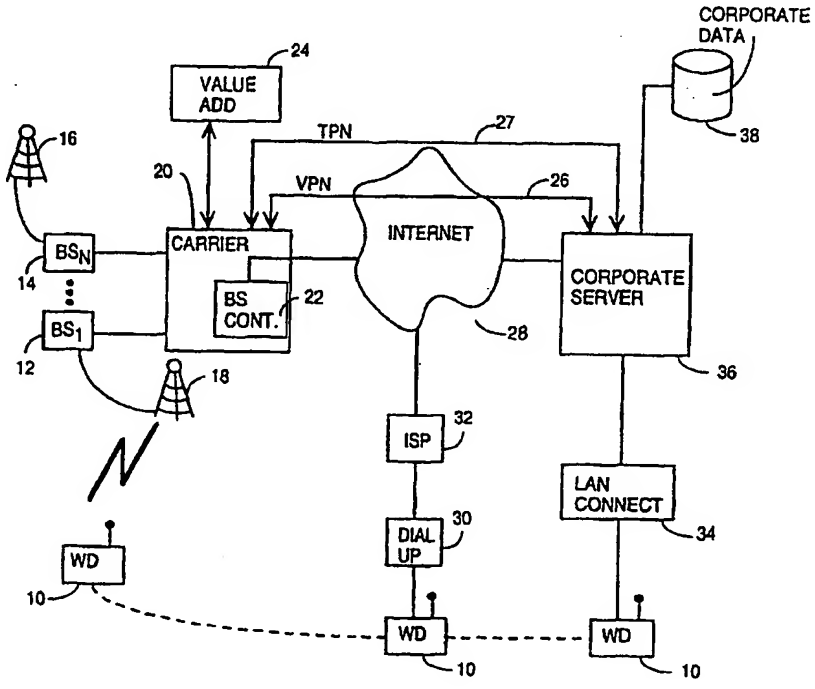
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A SYSTEM AND METHOD FOR MAINTAINING A VIRTUAL CONNECTION TO A NETWORK NODE

(57) Abstract

A wireless device (10) is provided with a plurality of connectivity options that enable it to connect to a carrier (20) via alternative connectivity routes thereby providing access to value-added (24) services and other information over plurality of connectivity routes (14). A user of the wireless device may select alternative connectivities when available based on dollar expense, available bandwidth, reliability, latency, or other considerations. Volume data delivery may be deferred until a more suitable connectivity route is established. With each change of connectivity the wireless device should reauthenticate itself. Reauthentification can be simplified by employing the previously authenticated route and leveraging the original authentication.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

A SYSTEM AND METHOD FOR MAINTAINING A VIRTUAL CONNECTION TO A NETWORK NODE

BACKGROUND OF THE INVENTION

(1) Field of the Invention

The invention relates to connectivity in a wireless network. More specifically, the invention relates to providing alternative connectivities and improved authentication between a carrier and a wireless device.

(2) Background

Wireless devices such as laptop computers, two-way pagers, palm PCs, personal digital assistants (PDAs), etc. have proliferated in recent years. Typically, these devices establish connectivity via a radio tower having an associated base station which communicates with a carrier. The carrier typically has a plurality of base stations associated therewith. Each base station covers a different though possibly overlapping segment of the carrier's coverage area. A wireless device is generally connected to no more than one base station at any time. The particular base station to be used is usually selected based on signal strength. When the signal strength from a different base station exceeds the signal strength of the base station through which the wireless device is currently communicating, a hand-off is performed and the new base station takes over providing a link to the carrier.

While the carrier itself may provide some information to the wireless device directly, often it is not the end of the communication pipe but rather acts as a proxy for the wireless device to gain access to other data available over other networks. The carrier is expected to have a reliable connection to such data and in turn funnels it to the wireless device. The carrier also may provide security and protocol conversion functions desirable in the wireless environment. The carrier may also maintain a

record of user preferences, display options, etc., such that data presented via the carrier arrives consistent with those preferences.

When connectivity is initially established, it is necessary for the wireless device to authenticate itself to the carrier. It can take minutes to complete the authentication process, the more extensive and secure the authentication process, the longer it usually takes. Once authenticated, the carrier may provide access to the Internet, a corporate server, or any number of other value-added services. The proliferation of wireless devices has similarly caused a proliferation in available value-added services. Unfortunately, such value-added services typically cease to be available to the wireless device when the wireless device is outside the coverage area of the carrier. Often, when a user is outside of the coverage area of their carrier, no option exists for obtaining access to the value-added services available within the coverage area at any cost.

Moreover, existing systems do not permit, for example, a user to access from their desktop PC the value-added services available through their wireless device. Thus, to obtain access to the value-added services, the wireless device continues to communicate via the base station to the carrier over the bandwidth constrained and relatively expensive wireless connectivity.

In view of the foregoing, it would be desirable to have an improved method and system which provides improved access to the carrier's value-added services. It would further be desirable to reduce the cost of authentication.

BRIEF SUMMARY OF THE INVENTION

A method and system for maintaining connectivity to a network node is disclosed. A wireless device is provided having a plurality of connectivity options. A carrier interfaces between the wireless device and information desired by the wireless device. The wireless device may carry on wireless communication with the carrier through a base station. When the wireless device communicates with the carrier through an alternative

connectivity, a virtual base station controller interfaces between the carrier and wireless device.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a system of one embodiment of the invention.

Figure 2 is a block diagram of a wireless device of one embodiment of the invention.

Figure 3 is a flow chart of an authentication routine of one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

A wireless device is provided with a plurality of connectivity options that enable it to connect to a carrier via alternative connectivity routes thereby providing access to value-added services and other information over a plurality of connectivity routes. A user of the wireless device may select alternative connectivities when available based on dollar expense, available bandwidth, reliability, latency, or other considerations. Volume data delivery may be deferred until a more suitable connectivity route is established. With each change of connectivity the wireless device should reauthenticate itself. Reauthentication can be simplified by employing the previously authenticated route and leveraging the original authentication.

Figure 1 is a block diagram of a system of one embodiment of the invention. A carrier 20 is coupled to a plurality of base stations (BS_1 - BS_N where N may be an arbitrarily large number). Each base station is coupled to a transceiver tower. BS_1 12 is coupled to transceiver tower 18, while BS_N 14 is coupled to transceiver tower 16. A wireless device 10 may communicate via a transceiver tower 18 through base station 12 through carrier 20 to access value added services and other information. Typically, wireless device 10 sends network packets over the airwaves using a network specific protocol to the transceiver tower 18 which then forwards the packets

along to base station 12 and then to carrier 20. Carrier 20 reformats the request in the network packet to be compatible with a network through which the information and value added services can be reached.

In this way, carrier 20 may provide value-added services 24 and provide those in the opposite direction via base station 12 through transceiver tower 18 to wireless device 10. In some situations value added services 24 may initiate contact with wireless device 10 through carrier 20. Additionally, a virtual private network (VPN) 26 or a true private network (TPN) 27 may exist between the carrier 20 and corporate server 36, which has access to corporate data 38. The carrier may also access the corporate server or other information over a wide-area network (WAN), such as the Internet 28.

In one embodiment of the invention, in addition to the wireless connectivity just described, wireless device 10 is capable of one or more alternative connectivities. This enables wireless device 10 to communicate with the carrier 20 by a lower cost connectivity route when available or permit connectivity where not otherwise in coverage. In this case, cost may be defined in terms of dollar expense, bandwidth, latency, reliability, etc. For example, wireless device 10 may connect through dial-up unit 30 to Internet Service Provider (ISP) 32 and access the carrier through the Internet 28. However, since the carrier 20 is only accustomed to communicating directly with the wireless device via the carrier's physical base stations 12, 14, a virtual base station controller 22 is provided to interface between the carrier 20 and the wireless device 10 when the wireless device 10 connects via an alternative connectivity.

In one embodiment, the wireless device 10 tunnels network packets inside, e.g., Transmission Control Protocol/Internet Protocol (TCP/IP) packets, via dial-up unit 30 through an Internet Service Provider (ISP) 32 over the Internet 28 to virtual base station controller 22. Virtual base station controller 22 then detunnels the network packet and provides it to the carrier 20. Significantly, the virtual base station controller can be built as a "bolt-on" unit, thereby minimizing the amount of architecture reworking required to handle legacy concerns. It is expected that while remaining

logically distinct, the virtual base station controller will over time migrate into the carrier, that embodiment being within the scope of virtual base station controller as used herein.

Alternatively, the wireless device 10 may be connected via a local area network (LAN) connect 34 which might be a docking station on the desktop or any other connection to the LAN. Again, network packets may be tunneled by the LAN connection over the corporate server through the Internet 28 using VPN 26 or via TPN 27 to virtual base station controller 22. Virtual base station controller 22 then detunnels the network packets and provides the packet to the carrier as though it had received it from a physical base station. Even when connecting over the LAN, the wireless device may be unable to access the corporate server directly. For example, if the corporate server is a Microsoft Windows NT server available from Microsoft Corporation of Redmond, Washington, it may require NT authentication that the wireless device cannot perform. The wireless device may still go through the carrier which can perform NT authentication on behalf of the wireless device.

When the wireless device 10 connects to an alternative connectivity, if the device is still in a coverage area of a physical base station, the carrier should be notified of the hand-off to the new connectivity. In this instance, the point of connection, be it dial-up unit 30 or LAN connect 34, becomes a virtual base station. A hand-off between physical base stations is based on signal strength. Thus, if wireless device 10 moves from where the signal strength from tower 16 is less than the signal strength from tower 18, a hand-off from BS_N 14 to BS_1 12 will be initiated. Similarly, when a wireless device connects up via an alternative connectivity route, virtual base station controller 22 should initiate a hand-off from the wireless connectivity. This may be done by indicating to the carrier that the signal strength over the alternative connectivity route is very strong.

The virtual base station controller 22 is responsible for registering and maintaining a unique association with a virtual base station to which the wireless device is connected. It ensures that data from the carrier are properly routed back to the appropriate virtual base station. The virtual

base station controller 22 maintains an association of a unique number such as a manufacturers serial number (MSN), an electronic serial number (ESN), or personal identification number (PIN) and an internet protocol address. The rest of the carrier's network is advised of the unique number but does not care about the address. The virtual base station controller 22 may ensure proper routing by monitoring all transactions on the carrier and claiming those directed to its virtual base stations, or the carrier could be required to target the virtual base stations explicitly. In this manner, from the carrier's perspective, when the wireless device communicates through an alternative connectivity route, it merely appears as though its device roamed to different base stations.

Figure 2 shows a wireless device of one embodiment of the invention. Wireless device 50 contains an application 52 which may, for example, be an e-mail program or any other application suitable for operation on a wireless device. Application 52 sends data to and receives data from a network specific protocol layer 54. Network specific protocol layer 54 arranges, formats, and sequences according to a network type implementing and/or carrier convention, then passes this data to router 66. Router 66 routes the data and protocol information to a stack corresponding to a connectivity in use based on control signal 56. For example, as shown, the data and protocol information may be forwarded to a radio stack 60 and out over antenna 64 or alternatively, to TCP/IP stack 58 which will tunnel the data and network protocol information within the TCP/IP packet and send it out over port 62 via, for example, a telephone link. Control signal 56 may be generated by combinational logic (not shown) which detects connection to alternate connectivites. While two possible connectivities are shown, it is contemplated that multiple connectivities are possible, including without limitation, satellite uplink connectivity, LAN connectivity, dial-up connectivity, and normal wireless connectivity. It is also within the scope and contemplation of the invention for the wireless device to provide different protocol packets for each of its connectivities, rather than tunneling network packets within the protocol of the particular connectivity employed.

Each time the wireless device changes its connectivity route, some level of reauthentication is required. This authentication helps to ensure that no fraudulent carrier has inserted itself into the conversation and that access over the alternative connectivity is permitted. Because full authentication procedures may require significant costs in terms of: i) connection time, often taking minutes to complete, ii) processing power representing a nontrivial battery drain, and (iii) possibly dollar expense, one embodiment of the invention employs an improved authentication method in switching between connectivities. **Figure 3** is a flow chart of an authentication routine of one embodiment of the invention. At functional block 102, a change of connectivity is initiated. The change may be moving from wireless connectivity to dial-up or any other form of connectivity supported by the wireless device, or the change could be from one of the other connectivities back to the wireless connectivity. A determination is made at decision block 124 whether the device is still in coverage with the previous connectivity. If the device is still in coverage, a datum is passed on the authenticated connectivity at functional block 106. If the device is not still in coverage, a determination is made if a previous datum passed to the wireless device has timed out at decision block 108. If the datum has not timed out or if real-time datum passage is possible, the wireless device then returns proof of receipt of the datum on the new connectivity at functional block 110. For example, the datum might be a secret randomly generated key. Then proof of receipt of the datum might be a one-way hash of the key or merely the key itself. If at decision block 108, the previous datum has timed out, the wireless device must perform full authentication before being granted access to the carrier. After full authentication or after return of proof of receipt at functional block 110, the new connectivity is treated as authenticated and communication may be commenced at functional block 114.

In one embodiment of the invention, the carrier periodically passes new keys over a fully authenticated connection to a connected wireless device. The key is deemed to be valid for a period of time. The period during which the key is valid may be assigned different priority levels such

various modifications and changes can be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense. Therefore, the scope of the invention should be limited only by the appended claims.

that the age of the key may restrict the quality of the authentication. For example, it may be determined that a key five minutes or less old entitles its holder to full access to the services of the carrier. A key from five to fifteen minutes old may entitle the holder to access to some level of lower priority carrier documents, and a key over fifteen minutes old may be timed out, and therefore invalid, not providing access to the carrier at all. There may, of course, be multiple levels of priority and the time frames for validity of keys may be varied as a design choice.

If the protocol requires simultaneous connection for real time reauthentication over the new route, when going from wired connection to wireless, some transition routine is used to signal that disconnection is about to occur. This allows the necessary key exchange to take place rather than merely pulling the plug and losing the authenticated connection. In this routine, the virtual base station controller may, for example, indicate to the carrier that its signal strength is deteriorating while passing the authentication datum. A physical base station with the strongest signal strength will then establish a connection. Proof of receipt of the authentication datum can be passed to the carrier over the new connection. The new route is thereby authenticated. If keys are intermittently passed to the wireless device and have a non-trivial valid period then explicit signaling in advance of disconnection may be avoided.

In an alternate embodiment of the invention, the carrier passes the datum on a new connectivity and proof of receipt is provided on the previously authenticated connectivity. Because interaction on the authenticated connectivity is still required for further communication on the new connectivity, the reliability on the authentication processed is maintained.

While most existing carriers do not support an ongoing connection over multiples connectivities, another alternate embodiment of the invention maintains connections over more than one connectivity when more than one connectivity is simultaneously supported by the carrier.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that

CLAIMS

What is claimed is:

1. A system comprising:

a wireless device having a plurality of connectivity options;

a carrier that provides an interface between the wireless device and desired information;

a base station through which the wireless device may establish wireless communication with the carrier; and

a virtual base station controller interfacing between the carrier and the wireless device when an alternative connectivity is employed.

2. The system of claim 1 wherein the wireless device tunnels a network packet over the alternative connectivity.

3. The system of claim 2 wherein the virtual base station controller detunnels the network packet and presents the network packet to the carrier and wherein the virtual base station controller maintains a record of a source of the network packet.

4. The system of claim 3 wherein the network packets are tunneled in TCP/IP packets.

5. The system of claim 4 wherein the TCP/IP packets are secured using virtual private network techniques.

6. The system of claim 1 wherein when the wireless device establishes a new connectivity, authentication is performed using a previously authenticated connectivity.

7. A method comprising:

establishing a new connection route to a carrier from a wireless device;

receiving a datum from the carrier over one of a previously authenticated connection route and the new connection route; and

sending proof of receipt of the datum to the carrier over the one of the new connection route and the previously authenticated route on which the datum was not received.

8. The method of claim 7 further comprising:

tunneling network packets to the carrier from the wireless device over the new connection route.

9. The method of claim 7 wherein the wireless device maintains connection to both the new connection route and the previous authentication connection route until authentication of the new connection route is complete.

10. The method of claim 7 wherein the datum is received after the new connection route is requested.

11. A method comprising:

periodically forwarding an authentication datum to a wireless device over an authenticated connectivity;

receiving a proof of receipt of the authentication datum after the wireless device changes to a new connectivity; and

treating the new connectivity as authenticated once the proof of receipt is received.

12. The method of claim 11 further comprising:

establishing a time limit during which the authentication datum is valid.

13. The method of claim 12 wherein the limit may vary depending on an information requested.

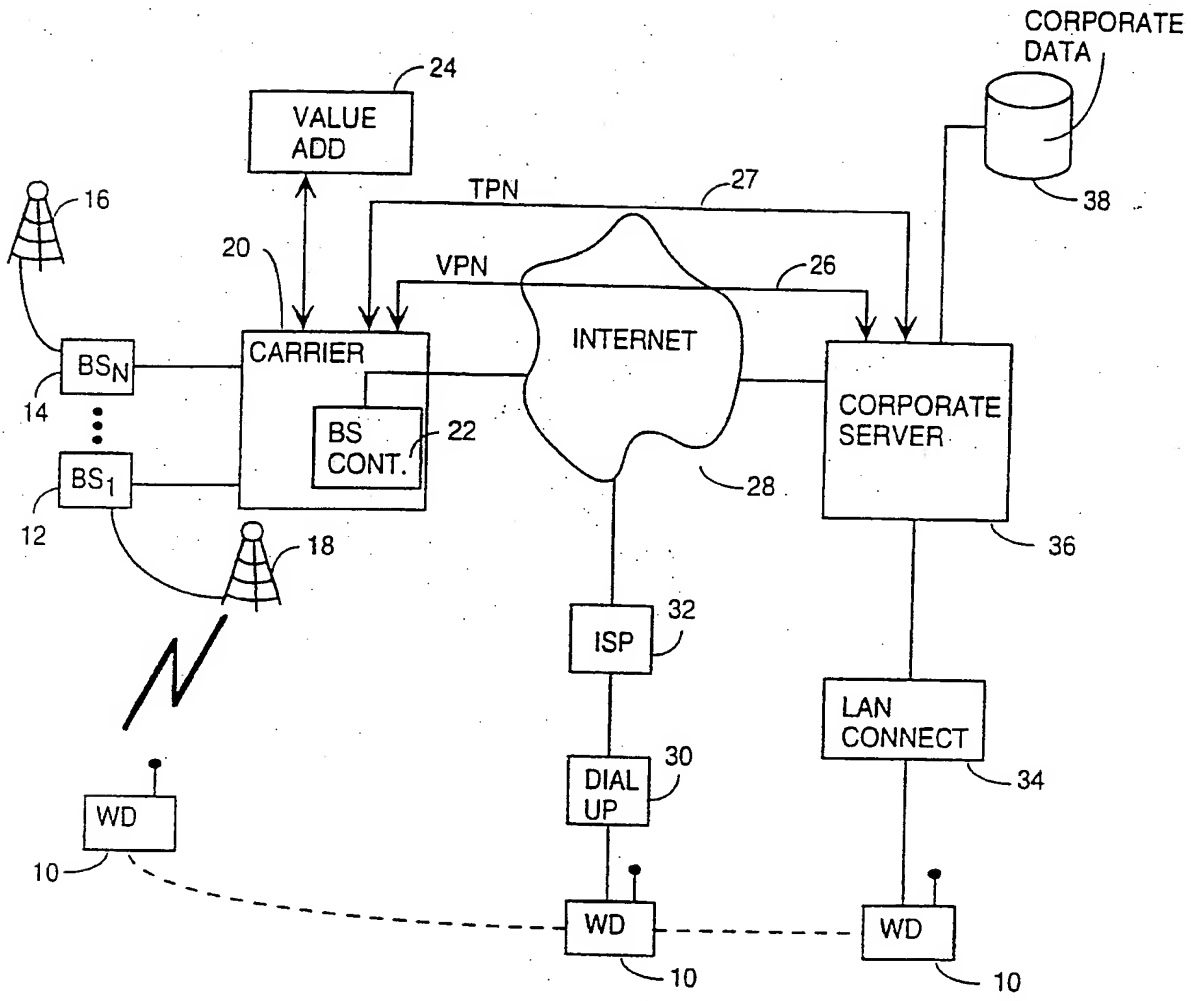

CORPORATE DATA
24
VALUE ADD
TPN
27
16
38
20
VPN
26
INTERNET
CARRIER
BS$_N$
CORPORATE SERVER
14
BS CONT.
22
BS$_1$
28
12
18
36
32
ISP
LAN CONNECT
30
DIAL UP
34
WD
10
WD
WD
10
10

Fig. 1

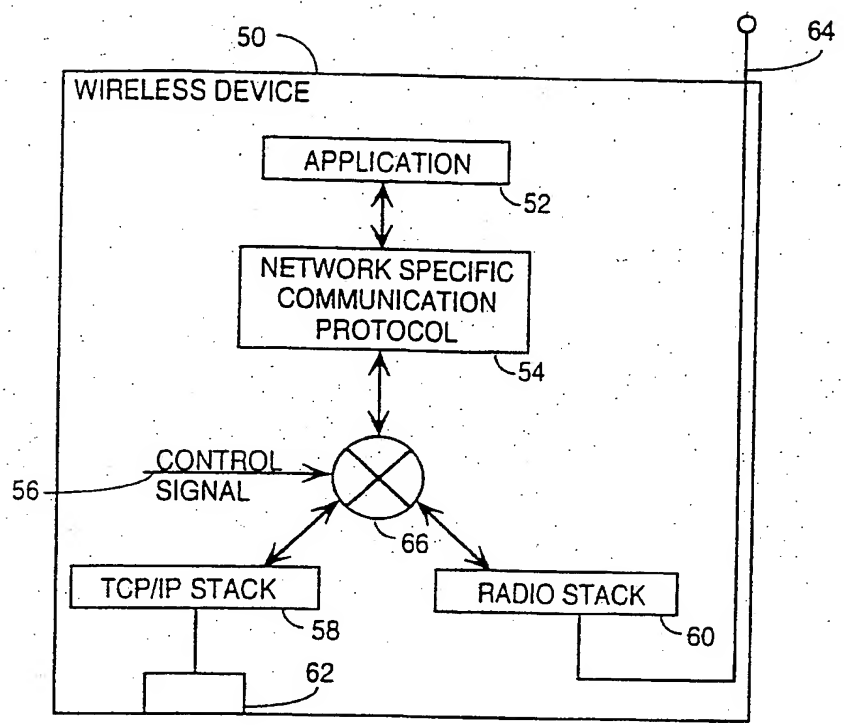

50
64
WIRELESS DEVICE
APPLICATION
52
NETWORK SPECIFIC COMMUNICATION PROTOCOL
54
CONTROL SIGNAL
56
66
TCP/IP STACK
58
RADIO STACK
60
62

Fig. 2

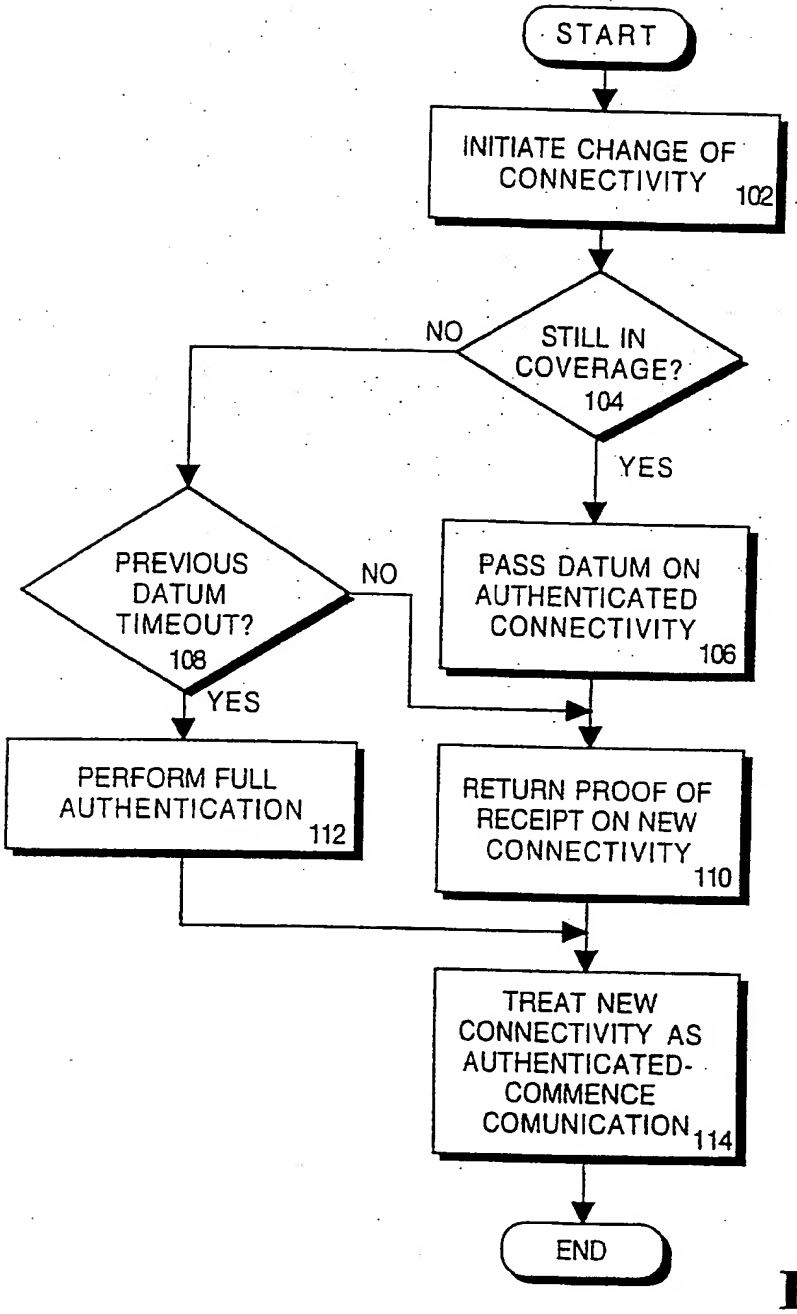

START
INITIATE CHANGE OF CONNECTIVITY 102
STILL IN COVERAGE? 104
NO
YES
PREVIOUS DATUM TIMEOUT? 108
NO
YES
PASS DATUM ON AUTHENTICATED CONNECTIVITY 106
PERFORM FULL AUTHENTICATION 112
RETURN PROOF OF RECEIPT ON NEW CONNECTIVITY 110
TREAT NEW CONNECTIVITY AS AUTHENTICATED-COMMENCE COMUNICATION 114
END

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/15174

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04Q 7/20
US CL :455/435; 380/23
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 455/435; 380/23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,894,478 A (BARZEGAR et al) 13 April 1999, col.1, lines 4564, col.2, lines 51-67, col.5, lines 43-56	1-13
Y,E	US 5,926,760 A (KHAN et al) 20 July 1999, col.6, lines 21-37, col.7, lines 29-62.	1-13
A	US 5,488,649 A (SCHELLINGER et al) 30 January 1996, col.4, lines 41-65, col.7, lines 7-37, col.12, lines 3-20.	1-13
A	US 5,668,875 A (BROWN et al) 16 September 1997, col.4, lines 28-55, col.6, lines 32-46, col.7, lines 34-65.	1-13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 AUGUST 1999	15 SEP 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 305-9711

Form PCT/ISA/210 (second sheet)(July 1992) ★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/15174

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS
search terms: wireless device,pager,cellular phone,authentication,base station,network,packets,datum,proof,receipt

Form PCT/ISA/210 (extra sheet)(July 1992) *